PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 12/14, 1/00, 9/32	A1	(11) International Publication Number: WO 00/42511
		(43) International Publication Date: 20 July 2000 (20.07.00)

(21) International Application Number: PCT/CA00/00021

(22) International Filing Date: 11 January 2000 (11.01.00)

(30) Priority Data:
2,258,338 11 January 1999 (11.01.99) CA

(71) Applicant *(for all designated States except US)*: CERTICOM CORP. [CA/CA]; 4th Floor, 5520 Explorer Drive, Mississauga, Ontario L4W 5L1 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: PEZESHKI, Farhad [AT/CA]; 10 Hope Street, Toronto, Ontario M6E 1J7 (CA). LAMBERT, Robert, J. [CA/CA]; 63 Holm Street, Cambridge, Ontario N3C 3N3 (CA).

(74) Agents: PILLAY, Kevin et al.; Orange Chari Pillay, Toronto Dominion Bank Tower, Suite 3600, Toronto-Dominion Centre, P.O. Box 190, Toronto, Ontario M5K 1H6 (CA).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR MINIMIZING DIFFERENTIAL POWER ATTACKS ON PROCESSORS

LINE#	SOURCE TEXT
1	TH = a random number between VMIN and VMAX
2	FOR V from VMIN to VMAX do
3	IF V < TH THEN
4	DO statements1 *{branch1}*
5	ELSE
6	DO statements2 *{branch2}*
7	OF

10

(57) Abstract

A method of masking a conditional jump operation in a cryptographic processor, wherein programm execution jumps to one of two branches dependent on a first or second condition of a distinguishing value V relative to a reference wherein the reference is bounded by an upper limit Vmax and a lower limit Vmin. The method comprising the steps of determining the location of a conditional jump and inserting code thereat for executing instructions to change program execution to a respective one of the two branches by using said distinguishing value and a base address to compute a target address, wherein for each evaluation of said condition a different number of instructions are